ABSTRACT OF THE DISCLOSURE

The present invention provides for trusted side-band communications between components in a computer system, so that use of the system bus may be avoided. Two components may be connected by means other than a bus (e.g., an infrared port, a wire, an unused pin, etc.), whereby these components may communicate without the use of the system bus. The non-bus communication channel may be referred to as "side-band." The side-band channel may be used to communicate information that might identify the user's hardware (e.g., a public key) or other information that the user may not want to be easily intercepted by the public at large. Communication over the side-band channel may also be used to verify that the participants in a communication are within a defined positional relationship to each other.